(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 December 2019 (26.12.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/246533 A1

(51) International Patent Classification:
G07F 7/10 (2006.01) *G06Q 20/40* (2012.01)
G07F 7/08 (2006.01) *G06Q 20/04* (2012.01)
G06Q 20/34 (2012.01)

(21) International Application Number:
PCT/US2019/038487

(22) International Filing Date:
21 June 2019 (21.06.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/014,542 21 June 2018 (21.06.2018) US

(71) Applicant: **CAPITAL ONE SERVICES, LLC** [US/US]; 1680 Capital One Drive, McLean, Virginia 22102 (US).

(72) Inventors: **OSBORN, Kevin**; 49 Hillside Road, Newton, Massachusetts 02461 (US). **KELLY, Kevin**; 5501 Prock Lane, Austin, Texas 78721 (US).

(74) Agent: **YOUNG SR., Michael V.**; Finnegan, Henderson, Farabow, Garrett & Dunner, LLP, 901 New York Avenue, NW, Washington, District of Columbia 20001-4413 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

WO 2019/246533 A1

(54) Title: SYSTEMS AND METHODS FOR SECURE READ-ONLY AUTHENTICATION

(57) Abstract: A system for authenticating a user with a mobile device comprising a memory storing instructions, and a processor in communication with a network. The processor may be configured to execute the stored instructions to receive, from a mobile device, an authentication request; obtain, from a database, a permanent identifier associated with a transaction card; generate a temporary identifier associated with the transaction card; generate an expected value by encrypting the permanent identifier and the temporary identifier; verify the expected value against an encrypted value received from the mobile device; and transmit an authorization command to the mobile device.

SYSTEMS AND METHODS FOR SECURE READ-ONLY AUTHENTICATION

RELATED APPLICATIONS

[001] This application claims priority to U.S. Patent Application No. 16/014,542, filed on June 21, 2018, the entire disclosure of which is incorporated by reference in the present application.

DESCRIPTION

Technical Field

[002] The disclosed embodiments generally relate to authenticating an account card and, more particularly, to authenticating an account card using a synchronized counter.

Background

[003] Many types of interactions on computer systems, such as authenticated log-ins and other transaction-based processes, are insecure. For example, when attempting to log in to a website on a computer, the website may request a username and password. Anyone with that set of information – be it an authorized user or a nefarious one – may use the website for any purpose. To combat this insecurity, some transactions require multi-factor authentication—often referred to as "what you know and what you have." For example, when logging into a website, the website may request a username/password combination ("what you know") along with a six-digit number displayed on an electronic device ("what you have") or a fingerprint scan ("who you are"). The six-digit number, also known as a time-based one-time password (TOTP), may change every 30 seconds so as to avoid reuse by an unauthorized user. As another example, a credit card may have information stored on it that can enable a credit card processor to know whether the card is physically present in the user's hands. For example, while the card may have a card number printed on the obverse ("what you know") some information may only be present as part of an EMV chip ("what you have"). Certain devices may read information from the EMV chip for contactless authentication of the user. Some devices allow multi-factor authentication using a "what you know" factor and a "who you are," e.g., a biometric such as face recognition, fingerprint verification, and/or iris scan.

[004] Currently EMV protocol relies on two-way communication between the EMV chip of the transaction card and a payment terminal, for example, at a point-of-sale (POS). To complete a transaction, transaction information is sent to the transaction card from the payment terminal. The EMV chip receives the transaction information, digitally signs the information, and transmits the signed information back to the payment terminal for verification. However, many devices and/or operating systems do not support two-way communication and therefore cannot complete transactions with EMV-enabled transaction cards.

[005] Due to these and other drawbacks associated with authentication using a two-way communication protocol, there exists a need for technology allowing secure, read-only authentication.

SUMMARY

[006] Consistent with disclosed embodiments, a transaction card associated with a financial account and for generating an encrypted value as part of an authentication request is provided. The transaction card comprises a radio frequency transmitter; a clock generator coupled to the radio frequency transmitter, the clock generator being configured to increment a counter value responsive to a wireless read signal received from an external radio frequency reader device; and a near field communication tag coupled to the radio frequency transmitter and storing a permanent identifier and the counter value. The near field communication tag may be configured, in response to the received read signal, to: generate an encrypted value based on the permanent identifier and the counter value; and provide the encrypted value to the radio frequency transmitter for transmission to the external radio frequency reader device.

[007] Consistent with another disclosed embodiment, a transaction card associated with a financial account and for generating an encrypted value as part of an authentication request is provided. The transaction card comprises a radio frequency transmitter; a near field communication tag coupled to the radio frequency transmitter; and a clock coupled to the near field communication tag and powered by a power source. The clock may be configured to send a time value to the near field communication tag responsive to a wireless read signal received by the near field communication tag from an external radio frequency reader device. The near field communication tag may be configured to: store a permanent identifier and the time value; and, in response to the received read signal, to: generate an encrypted value based on the permanent identifier and the time value; and provide the encrypted value to the radio frequency transmitter for transmission to the external radio frequency reader device.

[008] Consistent with another disclosed embodiment, a transaction card associated with a financial account and for generating an encrypted value as part of an authentication request is provided. The transaction card comprises: a radio frequency transmitter; a near field communication tag coupled to the radio frequency transmitter; and a microprocessor coupled to the near field communication tag and powered by a power source. The microprocessor may be configured to calculate an update value responsive to a wireless read signal received from an external radio frequency reader device. The near field communication tag may be configured to: store a permanent identifier and the update value, and in response to the received read signal: generate an encrypted value based on the permanent identifier and the update value, and provide the encrypted value to the radio frequency transmitter for transmission to the external radio frequency reader device.

[009] Consistent with other disclosed embodiments, tangible computer-readable storage media may store program instructions that are executable by one or more processors to implement any of the processes disclosed herein.

[010] It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only, and are not restrictive of the disclosed embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[011] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments and, together with the description, serve to explain the disclosed principles. In the drawings:

[012] Fig. 1 is a block diagram of an exemplary system, consistent with disclosed embodiments;

[013] Figs. 2A-2C are diagrams of exemplary transaction cards, consistent with disclosed embodiments;

[014] Figs. 3A-3C are flowcharts illustrating the incrementation of a temporary identifier, consistent with disclosed embodiments; and

[015] Fig. 4 is a flowchart of an exemplary process for authenticating a user with a transaction card having a polymorphic tag, consistent with disclosed embodiments.

DESCRIPTION OF THE EMBODIMENTS

[016] Reference will now be made in detail to exemplary embodiments, examples of which are illustrated in the accompanying drawings and disclosed herein. Wherever convenient, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

[017] In disclosed embodiments, a user may use a transaction card as a form of authentication when completing a financial transaction on a mobile device. The transaction card may be associated with a financial account held by the user with a financial service provider. Most transaction cards include static identifiers in one or more RFID tags or other storage components. However, such static identifiers are easily duplicated by nefarious users. Disclosed embodiments implement a transaction card including a dynamic polymorphic tag that changes each time the tag is read. This dynamic tag is more secure than traditional static tags and prevents nefarious users from simply duplicating and using the tag.

[018] The term "transaction card," as used herein, refers to any physical card product that is configured to provide information, such as financial information (e.g., card numbers, account numbers, account balance, etc.), quasi-financial information (e.g., rewards balance, discount information, etc.), and/or individual-identifying information (e.g., name, address, etc.), when the card is read by a card reader. Examples of transaction cards include credit cards, debit cards, gift cards, rewards cards, frequent flyer cards, merchant-specific cards, discount cards, etc., but are not limited thereto. The term "transaction card" may include an identification card such as a passport card, a driver's license, an entry point access card, or the like. The physical properties of the transaction card (e.g., size, flexibility, location of various components included in the card) may meet the various international standards, including, e.g., ISO/IEC 7810, ISO/IEC 7811, ISO/IEC 7812, ISO/IEC 7813, ISO/IEC 7816, ISO 8583, ISO/IEC 4909, and ISO/IEC 14443. For example, a transaction card may have a dimension of 85.60 mm (width) by 53.98 mm (height) by 0.76 mm (thickness), as specified in ISO/IEC 7810.

[019] Figure 1 shows a diagram of an exemplary system 100, consistent with disclosed embodiments. As shown in Figure 1, system 100 may include a user device 110, a transaction card 120, a network 130 to facilitate communication among the components of system 100, and a service provider (SP) device 140. The components and arrangement of the components included in system 100 may vary. Thus, system 100 may further include other components that perform or assist in the performance of one or more processes consistent with the disclosed embodiments. The components and arrangements shown in Figure 1 are not intended to limit the disclosed embodiments, as the components used to implement the disclosed processes and features may vary.

[020] System 100 may include one or more user devices 110. A user may operate a user device 110, which may be a desktop computer, laptop, tablet, smartphone, multifunctional watch, pair of multifunctional glasses, tracking device, or any suitable device with computing capability. User device 110 may include one or more processor(s) and memory device(s) known to those skilled in the art. For example, user device 110 may include memory device(s) that store data and software instructions that, when executed by one or more processor(s), perform operations consistent with the disclosed embodiments. In one aspect, user device 110 may have a transaction application installed thereon, which may enable user device 110 to communicate with transaction card 120 or SP device 140, via network 130 or via other means (e.g., a near-field communication device). For instance, user device 110 may be a smartphone or tablet or the like that executes a stored mobile application to perform various electronic transactions, such as authentication operations (e.g., logging into a computer system), banking operations (e.g., funds transfer, purchase, or cash withdrawal), or the like. In other embodiments, user device 110 may connect to SP device 140 through use of browser software stored and executed by user device 110. User device 110 may be configured to execute software instructions to allow a user to access information stored in SP device 140, such as, for example, private keys or other authentication information, financial information related to recent purchase transactions, financial discounts, financial statements, account information, rewards program information and the like. Additionally, user device 110 may be configured to execute software instructions that initiate and conduct transactions with SP device 140 and/or transaction card 120, such as, for example, a log-in or authentication, with a website or computer, cash withdrawals, wire transfers, PIN resets, or call center transactions.

[021] User device 110 may perform one or more operations consistent with the disclosed embodiments. User device 110 may be operated by a user. In one aspect, the user may be a customer of a financial service provider (e.g., a financial service provider operating SP device 140). For instance, a financial service provider may maintain a financial service account (e.g., checking account, savings account, debit card account, or credit card account) for the user of user device 110. User device 110 (and/or other items, such as a card, a token, a key fob, or the like) may access such an account to facilitate the purchase of goods, services, or information. Additionally or alternatively, user device 110 and the financial service account (for example, through a mobile application

installed on user device 110) may initiate the withdrawal of cash from an ATM, contact a customer call center, transfer or wire money, or reset their debit account PIN.

[022] In some embodiments, user device 110 may include an RFID reader, which may detect transaction card 120 using one or more wireless protocols (e.g., Near Field Communication (NFC), BLUETOOTH™, BLUETOOTH LE™ (BLE), Radio-Frequency Identification (RFID)). As explained below, transaction card 120 may include a polymorphic tag enabling the user to use transaction card 120 as a factor in a multi-factor authentication process. User device 110 may read an encryption of a tag and a "salt," that is, a piece of random data, stored on transaction card 120 and compare the encryption to an expected value stored on SP device 140.

[023] Transaction card 120 may be configured to transmit data using protocols such as BLUETOOTH™, BLUETOOTH LE™ (BLE), Wi-Fi, near field communications (NFC), or the like. In some embodiments, transaction card 120 may also comprise a wireless transmitter, e.g., RFID transmitter.

[024] In some embodiments, transaction card 120 may comprise one or more memory devices that store one or more identifiers. For example, transaction card 120 may store a tag, or permanent identifier, that uniquely identifies transaction card 120, as well as one or more other temporary/rolling identifiers, e.g., a salt value. For example, transaction card 120 may be configured to store a tag including a private key and a salt that is incremented each time the transaction card 120 is read by user device 110. Transaction card 120 may store the salt in memory (e.g., by overwriting a previously recorded salt). Transaction card 120 may comprise an RFID transmitter configured to send an encryption of the permanent identifier and temporary identifier to user device 110. In some embodiments, one or more identifiers may be stored in a database accessible to SP device 120.

[025] Consistent with disclosed embodiments, SP device 140 may be a system associated with a website, such as a secure data storage website that stores and provides data to users. SP device 140 may also be a system associated with a financial service provider (not shown), such as a bank, a credit card company, a lender, brokerage firm, or any other type of financial service entity that generates, provides, manages, and maintains financial service accounts, etc. for one or more users.

[026] SP device 140 may be implemented as one or more computing systems that are configured to execute software instructions stored on one or more memory devices to perform one or more operations consistent with the disclosed embodiments. For example, SP device 140 may include one or more memory device(s) storing data and software instructions, and one or more processor(s) configured to use the data and execute the software instructions to perform server-based functions and operations known to those skilled in the art. SP device 140 may include one or more general purpose computers, mainframe computers, or any combination of these types of components.

[027] In certain embodiments, SP device 140 may be configured as a particular apparatus, system, and the like based on the storage, execution, and/or implementation of the software instructions that cause a processor to perform one or more operations consistent with the disclosed

embodiments. SP device 140 may be standalone, or it may be part of a subsystem, which is in turn part of a larger system. For example, SP device 140 may represent distributed servers that are remotely located and communicate over a public network (e.g., network 140) or a dedicated network, such as a LAN, for a financial service provider.

[028] SP device 140 may include or may access one or more storage devices configured to store data and/or software instructions used by one or more processors of SP device 140 to perform operations consistent with disclosed embodiments. For example, SP device 140 may include a memory configured to store one or more software programs that performs several functions when executed by a processor. The disclosed embodiments are not limited to separate programs or computers configured to perform dedicated tasks. For example, SP device 140 may include memory that stores a single program or multiple programs. Additionally, SP device 140 may execute one or more programs located remotely from SP device 140. For example, SP device 140 may access one or more remote programs stored in memory included with a remote component that, when executed, perform operations consistent with the disclosed embodiments. In certain aspects, SP device 140 may include server software that generates, maintains, and provides services associated with financial account management. In other aspects, SP device 140 may connect separate server(s) or similar computing devices that generate, maintain, and provide services associated with financial data for a financial service provider associated with SP device 140.

[029] SP device 140 may be configured to generate and send an expected value to user device 110. The expected value may correspond to the tag and salt of the transaction card 120. SP device 140 may also be connected to a database and may store generated tag and salt pairs associated with one or more transaction cards 120.

[030] Network 130 may comprise any type of computer networking arrangement used to exchange data. For example, network 130 may be one or more of the Internet, a private data network, a virtual private network over a public network, a Wi-Fi network, a LAN or WAN network, and/or other suitable connections that may enable information exchange among various components of the system 100. Network 130 may also include a public switched telephone network ("PSTN") and/or a wireless cellular network. Network 130 may be a secured network or unsecured network. In other embodiments, one or more components of system 100 may communicate directly through a dedicated communication link(s), such as links between user device 110 and service provider device 140.

[031] Additionally or alternatively, network 130 may include a direct communication network. Direct communications may use any suitable technologies, including, for example, BLUETOOTH™, BLUETOOTH LE™ (BLE), Wi-Fi, near field communications (NFC), or other suitable communication methods that provide a medium for transmitting data between separate devices. In certain embodiments, user device 110 may connect and communicate through a direct communications network.

[032] Other components known to one of ordinary skill in the art may be included in system 100 to process, transmit, provide, and receive information consistent with the disclosed embodiments.

[033] Figure 2A is a diagram of an exemplary transaction card 200A, which may correspond to transaction card 120 (Fig. 1) consistent with disclosed embodiments. Card 200A may include a clock generator 201, an NFC tag 202, and an RFID transmitter 203.

[034] Clock generator 201 may be configured to cycle on in response to electromagnetic emissions from an RFID reader. For example, transaction card 200A may include a Javacard chip, including NFC tag 202, using ISO 14443, such that clock generator 201 may cycle on upon receipt of a signal having a frequency of 13.56 mHz from an RFID reader. Each time clock generator 201 cycles on, a counter may be incremented by a preconfigured value unique to the transaction card. Thus, clock generator 201 may be configured to "clock" each read of the transaction card 120 by an RFID reader. The starting value of the counter may also be a unique, preconfigured, non-zero value. Clock generator 201 may be any configuration of clock generator circuitry known to one of skill in the art.

[035] NFC tag 202 may be a chip including an antenna and an integrated circuit (IC). In some embodiments NFC tag 202 may be an RFID tag. In another embodiment, NFC tag 202 may be a component of a microchip or microcontroller operating via NFC coil. In some embodiments, transaction card 200A may include a microchip (e.g., EMV chip), a communication device (e.g., Near Field Communication (NFC) antenna, Bluetooth® device, WiFi device), a magnetic strip, a barcode, a Quick Response (QR) code, and/or other devices in addition to, or instead of, NFC tag 202. In some embodiments, NFC tag 202 may be a component of a Javacard chip operating under the ISO 14443 standard.

[036] In some embodiments, NFC tag 202 may store information comprising a permanent identifier and a temporary identifier, also referred to as a tag and a salt, respectively. The permanent identifier may comprise an identification number unique to the user. In some embodiments, the permanent identifier may be an identification number unique to the transaction card. In another embodiment, the permanent identifier comprises transaction data stored by NFC tag 202. For example, a merchant ID for the past one, two, three, etc. transactions. In other embodiments, stored transaction data may include transaction type, merchant ID, transaction amount, or any combination thereof. The temporary identifier may be data, for example, a numerical value, that may be appended to the permanent identifier. Upon detecting an electromagnetic signal emitted from an RFID reader, e.g., an RFID reader disposed in a mobile device, a current may be induced in a coil of NFC tag 202, thereby powering clock generator 201 to cycle on, causing the temporary identifier to increase by the preconfigured increment. The NFC tag 202 then generates an encryption of the permanent identifier and the incremented temporary identifier. In some embodiments, the encryption may comprise a hash of the permanent identifier and the incremented temporary identifier.

[037] RFID transmitter 203 may be configured to transmit the encrypted value to a device, e.g., user device 110. RFID transmitter 203 may be part of NFC tag 202 and may be configured to transmit the encrypted value to an RFID reader responsive to a signal received from the reader. RFID transmitter 203 may further be configured to transmit encrypted transaction card data to user device 110.

[038] For example, with reference to Figure 3A, at a first cycle, NFC tag 202 may detect a signal from an RFID reader, which induces a coil of NFC tag 202. NFC tag 202 may supply power generated by the induction of said coil to clock generator 201 (step 301). Each clock cycle begins upon the receipt of power from NFC tag 202. For example, receipt of a supply of power from NFC tag 202 may initiate clock cycle 1, clock cycle 2, ... clock cycle n. In response, clock generator 201 may return a signal 302 to the NFC tag 202. At step 303, in response to the receipt of signal 302, NFC tag 202 may increment the counter 305 by a value N to generate a salt in the form of a temporary identifier C1. In some embodiments, N may be an integer value. N and/or the initial counter value may be unique to the transaction card 200A. At step 304, NFC tag 202 may then append this salt C1, e.g., the counter + N, to the permanent identifier 306, e.g., the tag and generate an encryption of (PI + C1). NFC tag 202 may store C1 as the new counter value.

[039] The above process is repeated each time NFC tag 202 receives a signal from an RFID reader. In parallel, SP device 140 may receive an indication from user device 110 that a mobile application initiated an RFID reader. The SP device 140 may store the permanent identifier, initial counter value, and increment value. The SP device 140 may increment the counter each time information is received from user device 110 indicating that the RFID reader was initiated. When a user requests authentication via user device 110, the RFID reader of the device may receive, from RFID transmitter 203, the encrypted value generated by NFC tag 202 and send the encrypted value to SP device 140. To authenticate the user, SP device 140 may verify the encrypted value by comparing the encrypted value from the transaction card 200A with the encrypted value generated by the SP device 140.

[040] In some embodiments, the counter value of the transaction card may become out of sync with the counter value of the SP device. For example, if the transaction card was not successfully read, user device 110 may not communicate with SP device 140 to increment the counter. However, even if the transaction card is not read, NFC tag 202 may receive a signal from the RFID reader causing the counter to increment. In some embodiments, if the transaction card 120 is out of sync with SP device 140, SP device 140 may instruct the user, via user device 110, to tap the card a certain number of times to the mobile device 110, thereby generating a certain number of reads of the card causing the counter 305 of the card to increment. SP device 140 may determine that the sequence of encrypted values generated by performing the certain number of taps matches the expected sequence of encrypted values. If the sequence matches, SP device 140 may cause user device 110 to send instructions to transaction 120 to reset.

[041] The system may include a threshold number of cycles by which the NFC tag 202 and SP device 140 can be out of sync. For example, an innocent action, such as suboptimal card placement or an aborted attempt, may cause the transaction card and SP device to fall out of sync. A threshold number may be set such that, as long as the counter values match within the threshold number of cycles, the user may be authenticated. In this embodiment, the counter value of the card will be set as the current counter value of the SP device if it is within the threshold number of cycles. In another example, the counter may fall out of sync as a result of fraudulent activity. If the counters do not match within the threshold number of cycles, the authentication request may be denied and a fraud alert may be sent to the user and/or financial service provider. Additionally, this method of authentication protects against fraud because even if the encryption of the permanent identifier and temporary identifier is copied, a nefarious user would be unable to replay the copied encrypted value and be authenticated by the system.

[042] Figure 2B is a diagram of another exemplary card 200B, which may correspond to transaction card 120 (Fig. 1) consistent with disclosed embodiments. Transaction card 200B may include an NFC tag 202 and RFID transmitter 203, as well as a real time clock (RTC) 204 powered by a power source 205.

[043] RTC 204 may be an integrated circuit configured to keep accurate time. That is, RTC 204 may cycle on each second, thereby incrementing the stored time. When NFC tag 202 receives a signal from an RFID reader, RTC 204 may respond by sending a timestamp to NFC tag 202 such that the timestamp may be appended to the permanent identifier. In another embodiment, the timestamp may be appended to a numerical value. For enhanced user security, RTC 204 may be set to a unique starting time for each transaction card such that the timestamp at a given moment is different for each card.

[044] For example, with reference to Figure 3B, upon receiving a read from an RFID reader and inducing a current in the IC of NFC tag 202, NFC tag 202 sends a ping 301 to RTC 204. In response, RTC 204 initiates Cycle 1 and sends a signal 302 including the current timestamp, Time 1, to NFC tag 202. NFC tag 202, at step 303, appends current time stamp Time 1 to an identifier 307 unique to the transaction card to generate salt C1. At step 304, NFC tag 202 appends C1 to the permanent identifier 306 associated with the transaction card and generates an encrypted value of the PI + C1. In some embodiments, the encrypted value may be a hash of the PI + C1. In some embodiments, the timestamp may itself be the salt and may be directly appended to the PI 306 without first being appended and/or added to an identifier 307. The generated encrypted value may be compared to an encrypted value of the permanent identifier and the timestamp at the first clock cycle generated by SP device 140. If the encrypted values match, the user may be authenticated. RTC 204 of transaction card 200B and a corresponding RTC of SP device 140 may be synced by initiating both RTC's to the same time. In this embodiment, because the temporary identifier, e.g., salt, at any given clock cycle is only valid during a brief time period, the authentication by transaction card 200B is highly secure. For example, the encrypted value may be valid for a

predetermined window of time, e.g., 30 seconds, 60 seconds, etc. In some embodiments, to account for drift between the server clock and RTC 204, the system may accept a certain number of values before and after the current accepted value. While the use of an RTC to generate a salt is highly secure, RTC 204 requires a power source 205, e.g., a battery or other power source, to operate accurately.

[045] Figure 2C is a diagram of yet another exemplary card 200C, which may correspond to transaction card 120 (Fig. 1) consistent with disclosed embodiments. Transaction card 200C may include an NFC tag 202 and RFID transmitter 203, as well as a microprocessor 206 powered by a power source 205, e.g., a battery.

[046] Microprocessor 206 may be, for example, a microprocessor from the Pentium™ or Xeon™ family manufactured by Intel™, the Turion™ family manufactured by AMD™, or any of various processors manufactured by Sun Microsystems. In other embodiments, microprocessor 206 may be a programmable logic device. Microprocessor 206 may be configured to implement an algorithm such that the counter stored by NFC tag 202 is incremented by a different value at each clock cycle.

[047] Figure 3C is a simplified example of a series of clock cycles. As previously described, NFC tag 202 sends a ping 301 to microprocessor 206 upon receipt of a signal from an RFID reader. Microprocessor 206 responds by sending the result of the application of an algorithm to X to NFC tag 202. For example, microprocessor 206 may be configured such that a value X is divided by the number of the clock cycle. Thus, at a first clock cycle, Cycle 1, the counter 305 is incremented by X/1 to generate a temporary identifier, e.g., salt, C1 (step 303). At Cycle 2, the salt C1 generated during Cycle 1 is incremented by X/2 to generate salt C2, and so on. More complex algorithms may be implemented to generate the temporary identifier at each clock cycle. At step 304, NFC tag 202 appends the salt generated at step 303 to the permanent identifier 306 associated with the transaction card and determines an encrypted value of the permanent identifier 306 and the salt. Depending on the desired complexity, the algorithm stored by the processor may be directly applied to counter 305. In other embodiments, the result of the algorithm may be the temporary identifier, C1. As previously described, the user may be authenticated by verifying the encrypted value generated at step 304 with an expected encrypted value generated by SP device 140.

[048] In some embodiments, if the transaction card 120 and SP device 140 fall out of sync, SP device 140 may send instructions to user device 110 to send a signal to NFC tag 202 to reset the counter. In some embodiments, the user may be required to provide several authentication factors before resetting the NFC tag 202. When NFC tag 202 is reset, the counter or RTC may be set to its initial starting value. In other embodiments, for increased security, the counter or RTC may be set to a value different from the starting value. In another embodiment, user device 110 may transmit a new algorithm to microprocessor 206 or may alter the increment by which the counter (see, Fig. 3A) is increased.

[049] Figure 4 is a flowchart depicting an exemplary process 400 for authenticating a user with a transaction card having a polymorphic tag.

[050] At step 401, system 100 receives, at SP device 140, a request for authentication from user device 110. In some embodiments, the request for authentication may be made in connection with, for example, a purchase, transfer, or payment via a mobile application of the financial service provider. The financial service provider may require one or more factors to authenticate the user. The authentication request may include identifying information such as user ID, account number, etc. to associate the user with a transaction card.

[051] At step 402, SP device 140 obtains, from a memory or database, a permanent identifier associated with the transaction card. In some embodiments the permanent identifier is a private key.

[052] At step 403, SP device 140 generates a temporary identifier. The temporary identifier may be generated using any of the above methods described with reference to Figs. 3A-3C.

[053] At step 404, SP device 140 generates an encryption of the permanent identifier and the temporary identifier.

[054] At step 405, SP device 140 receives, via network 130, an encryption value from user device 110. The encryption value may be obtained from transaction card 120 via an RFID reader of user device 110.

[055] At step 406, the SP device 140 verifies the generated encryption value against the received encryption value. In some embodiments, verification may include a comparison of the encryption values. If the values are equal, the user may be authenticated. In some embodiments, SP device 140 may store expected encryption values associated with one or more clock cycles up to a threshold number of clock cycles. Thus, in some embodiments, if the received encryption value matches any of the values, the user may be authenticated.

[056] At step 407, SP device 140 may transmit an authentication command to the mobile device associated with the user. For example, SP device 140 may transmit, via network 130, instructions causing the mobile device to complete the transaction requiring authentication by the user.

[057] In some embodiments, a transaction card associated with a financial account and for generating an encrypted value as part of an authentication request is provided. The transaction card may include a radio frequency transmitter; a clock generator coupled to the radio frequency transmitter, the clock generator being configured to increment a counter value responsive to a wireless read signal received from an external radio frequency reader device; and a near field communication tag coupled to the radio frequency transmitter and storing a permanent identifier and the counter value. The near field communication tag may be configured, in response to the received read signal, to: generate an encrypted value based on the permanent identifier and the counter value; and provide the encrypted value to the radio frequency transmitter for transmission to the external radio frequency reader device.

[058] The permanent identifier may include a private key.

[059] The radio frequency transmitter may be configured to generate a digital signal when the clock generator cycles on.

[060] The clock generator may be configured to increment the counter value by a preconfigured amount when the clock generator cycles on. The clock generator may also be configured to update a temporary identifier, a numerical value, and the incremented counter value when the clock cycle generator cycles on. The numerical value may be unique to the transaction card. The near field communication tag may be configured to generate the encrypted value based on the permanent identifier, the counter value, and the numerical value. The near field communication tag may also be configured to store the numerical value after transmissions by the radio frequency transmitter.

[061] In some embodiments, the transaction card may include a radio frequency transmitter; a near field communication tag coupled to the radio frequency transmitter; and a clock coupled to the near field communication tag and powered by a power source. The clock may be configured to send a time value to the near field communication tag responsive to a wireless read signal received by the near field communication tag from an external radio frequency reader device. The near field communication tag may be configured to: store a permanent identifier and the time value; and, in response to the received read signal, to: generate an encrypted value based on the permanent identifier and the time value; and provide the encrypted value to the radio frequency transmitter for transmission to the external radio frequency reader device.

[062] The power source may include a battery. The power source may supply power to at least one of the radio frequency transmitter or the near field communication tag.

[063] The time value may include a timestamp of the clock. The time value may include the timestamp and a numerical value unique to the transaction card. The time value ~~may be~~ valid only during a preconfigured time period.

[064] In another embodiment, the transaction card may include: a radio frequency transmitter; a near field communication tag coupled to the radio frequency transmitter; and a microprocessor coupled to the near field communication tag and powered by a power source. The microprocessor may be configured to calculate an update value responsive to a wireless read signal received from an external radio frequency reader device. The near field communication tag may be configured to: store a permanent identifier and the update value, and in response to the received read signal: generate an encrypted value based on the permanent identifier and the update value, and provide the encrypted value to the radio frequency transmitter for transmission to the external radio frequency reader device.

[065] The near field communication tag may be configured to generate a temporary identifier based on the update value while the radio frequency transmitter is transmitting.

[066] The microprocessor may be further configured to vary the update value between subsequent transmissions. The update value may be calculated based on an algorithm. The algorithm may be unique to the transaction card.

[067] The transaction card may further include a memory component coupled to the microprocessor.

[068] The exemplary disclosed embodiments describe systems and methods for authenticating a user with a transaction card comprising a polymorphic tag. The foregoing description has been presented for purposes of illustration. It is not exhaustive and is not limited to the precise forms or embodiments disclosed. Modifications and adaptations of the embodiments will be apparent from consideration of the specification and practice of the disclosed embodiments. For example, the described implementations include hardware and software, but systems and methods consistent with the present disclosure can be implemented as hardware alone.

[069] Computer programs based on the written description and methods of this specification are within the skill of a software developer. The various programs or program modules can be created using a variety of programming techniques. For example, program sections or program modules can be designed in or by means of Java, C, C++, assembly language, or any such programming languages. One or more of such software sections or modules can be integrated into a computer system, computer-readable media, or existing communications software.

[070] Moreover, while illustrative embodiments have been described herein, the scope includes any and all embodiments having equivalent elements, modifications, omissions, combinations (e.g., of aspects across various embodiments), adaptations or alterations based on the present disclosure. The elements in the claims are to be interpreted broadly based on the language employed in the claims and not limited to examples described in the present specification or during the prosecution of the application, which examples are to be construed as non-exclusive. Further, the steps of the disclosed methods can be modified in any manner, including by reordering steps or inserting or deleting steps.

[071] Furthermore, although aspects of the disclosed embodiments are described as being associated with data stored in memory and other tangible computer-readable storage mediums, one skilled in the art will appreciate that these aspects can also be stored on and executed from many types of non-transitory computer-readable media, such as secondary storage devices, like hard disks, floppy disks, or CD-ROM, or other forms of RAM or ROM.

[072] It is intended, therefore, that the specification and examples be considered as example only, with a true scope and spirit being indicated by the following claims and their full scope of equivalents.

WHAT IS CLAIMED IS:

1. A transaction card comprising:

a radio frequency transmitter;

a clock generator coupled to the radiofrequency transmitter and having a dynamic frequency configured to cycle on while the transmitter is transmitting and to cycle off while the transmitter is not transmitting; and

a near field communication tag coupled to the clock generator and storing a permanent identifier and a temporary identifier, the temporary identifier comprising a numerical value and a counter value.

2. The transaction card of claim 1, wherein the permanent identifier comprises a private key.

3. The transaction card of claim 1, wherein the radio frequency transmitter is configured to generate a digital signal when the clock generator cycles on.

4. The transaction card of claim 1, wherein the near field communication tag is configured to increment the counter by a preconfigured amount when the clock cycle generator cycles on.

5. The transaction card of claim 4, wherein the near field communication tag is configured to update the temporary identifier the numerical value and incremented counter value when the clock cycle generator cycles on.

6. The transaction card of claim 1, wherein the numerical value is unique to the transaction card.

7. The transaction card of claim 1, wherein the near field communication tag is configured to generate an encryption of the permanent identifier and the temporary identifier.

8. The transaction card of claim 4, wherein the near field communication tag is configured to store the temporary identifier after transmissions by the radio frequency transmitter.

9. A transaction card comprising:

a radiofrequency transmitter;

a near field communication tag coupled to the radiofrequency transmitter; and

a real time clock coupled to the near field communication tag and powered by a power source, wherein:

the near field communication tag is configured to store a permanent identifier and a temporary identifier; and

the near field communication tag is configured to increment the temporary identifier by a value of the real time clock when the radiofrequency transmitter is transmitting.

10. The transaction card of claim 9, wherein the power source comprises a battery.

11. The transaction card of claim 9, wherein the value comprises a timestamp of the real time clock.

12. The transaction card of claim 11, wherein the value comprises the timestamp and a numerical value unique to a user of the transaction card.

13. The transaction card of claim 9, wherein the temporary identifier is valid only during a preconfigured time period.

14. The transaction card of claim 9, wherein the power source supplies power to at least one of the radiofrequency transmitter or the near field communication tag.

15. A transaction card comprising:

a radiofrequency transmitter;

a near field communication tag coupled to the radiofrequency transmitter and configured to store a permanent identifier and a temporary identifier; and

a microprocessor coupled to the near field communication tag and powered by a power source, the microprocessor being configured to calculate update values upon transmissions by the transmitter.

16. The transaction card of claim 15, wherein the near field communication tag is configured to increment the temporary identifier by one of the update values while the radiofrequency transmitter is transmitting.

17. The transaction card of claim 15, wherein the microprocessor is further configured to vary the update values between subsequent transmissions.

18. The transaction card of claim 15, wherein the update values are calculated based on an algorithm.

19. The transaction card of claim 18, wherein the algorithm is unique to a user associated with the transaction card.

20. The transaction card of claim 15 further comprising a memory component coupled to the microprocessor.

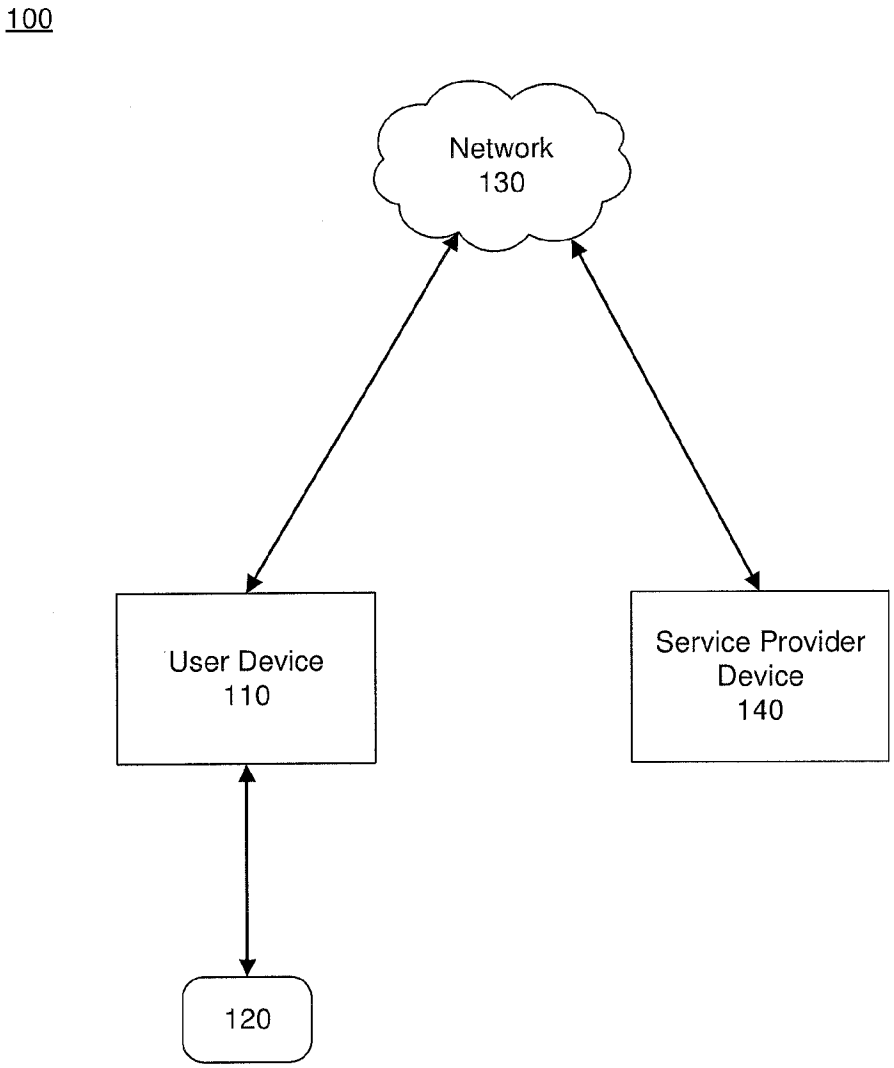
100
Network
130
User Device
110
Service Provider
Device
140
120

FIGURE 1

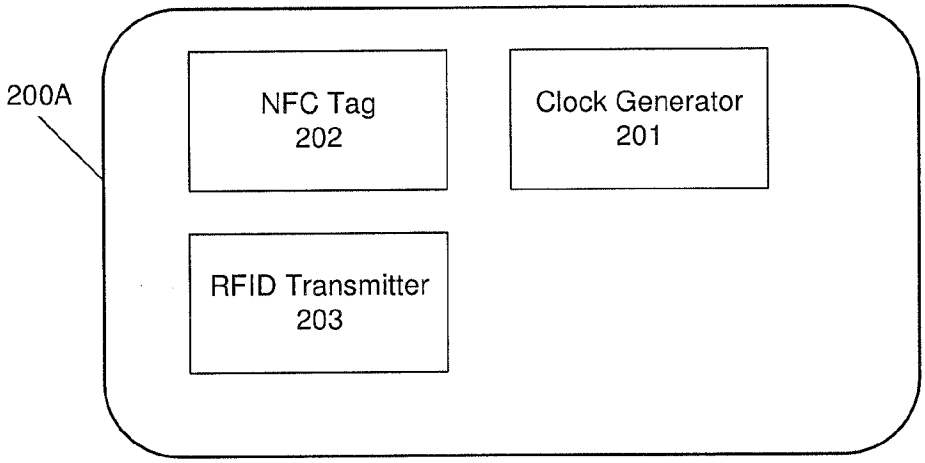

FIGURE 2A

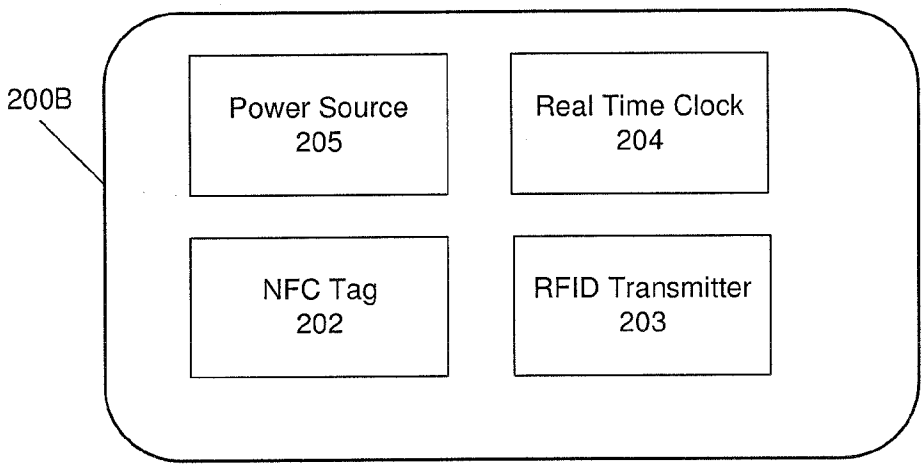

FIGURE 2B

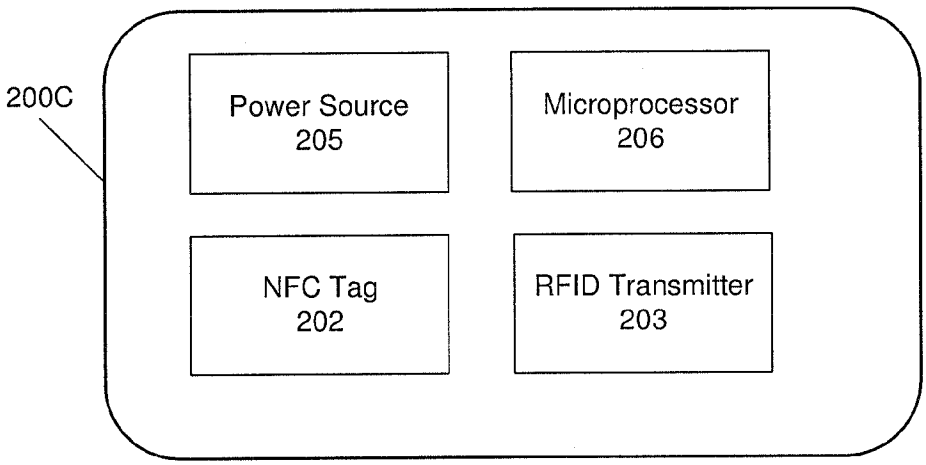
200C
Power Source
205
Microprocessor
206
NFC Tag
202
RFID Transmitter
203

FIGURE 2C

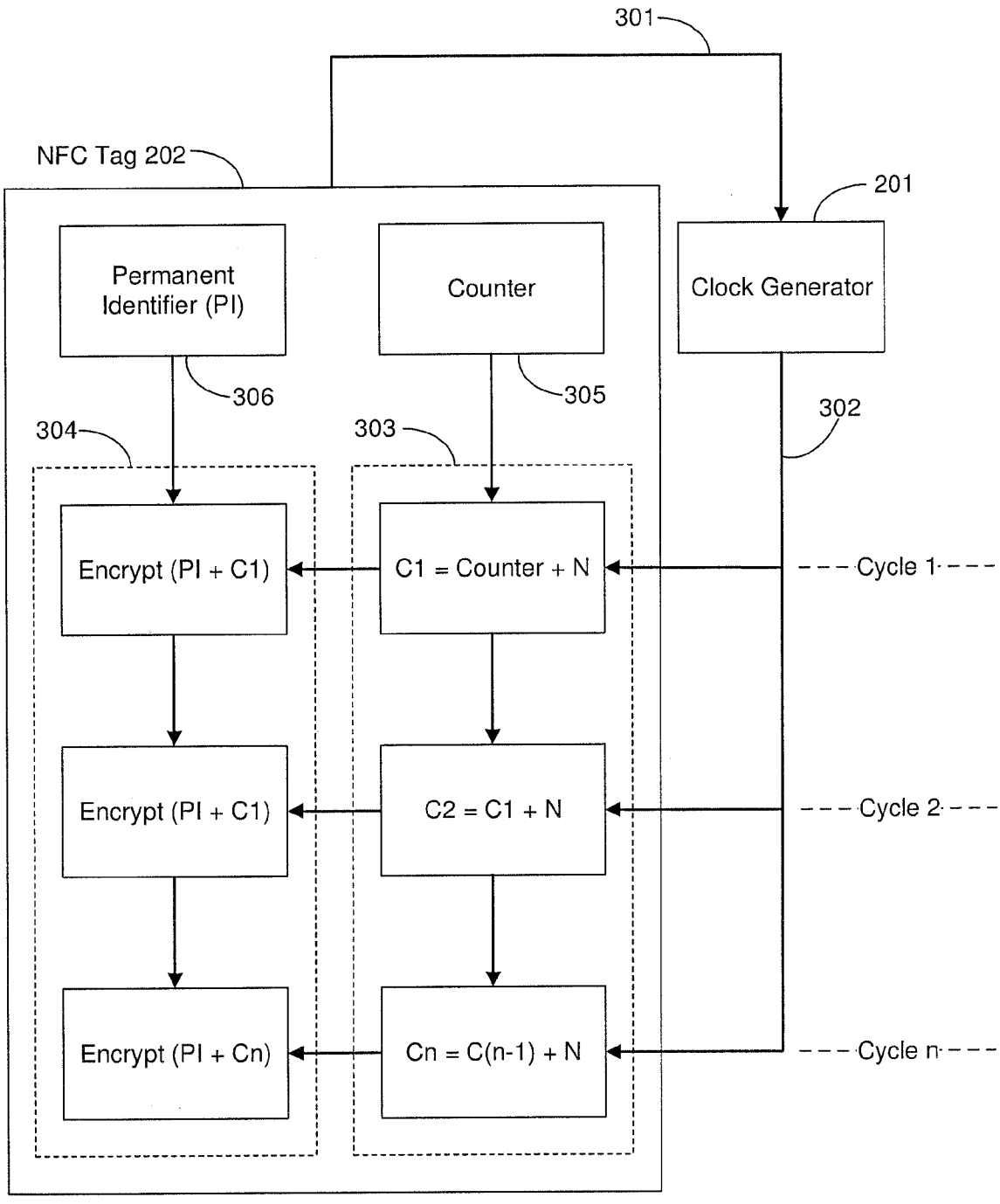
301
NFC Tag 202
201
Permanent Identifier (PI)
Counter
Clock Generator
306
305
302
304
303
Encrypt (PI + C1)
C1 = Counter + N
Cycle 1
Encrypt (PI + C1)
C2 = C1 + N
Cycle 2
Encrypt (PI + Cn)
Cn = C(n-1) + N
Cycle n

FIGURE 3A

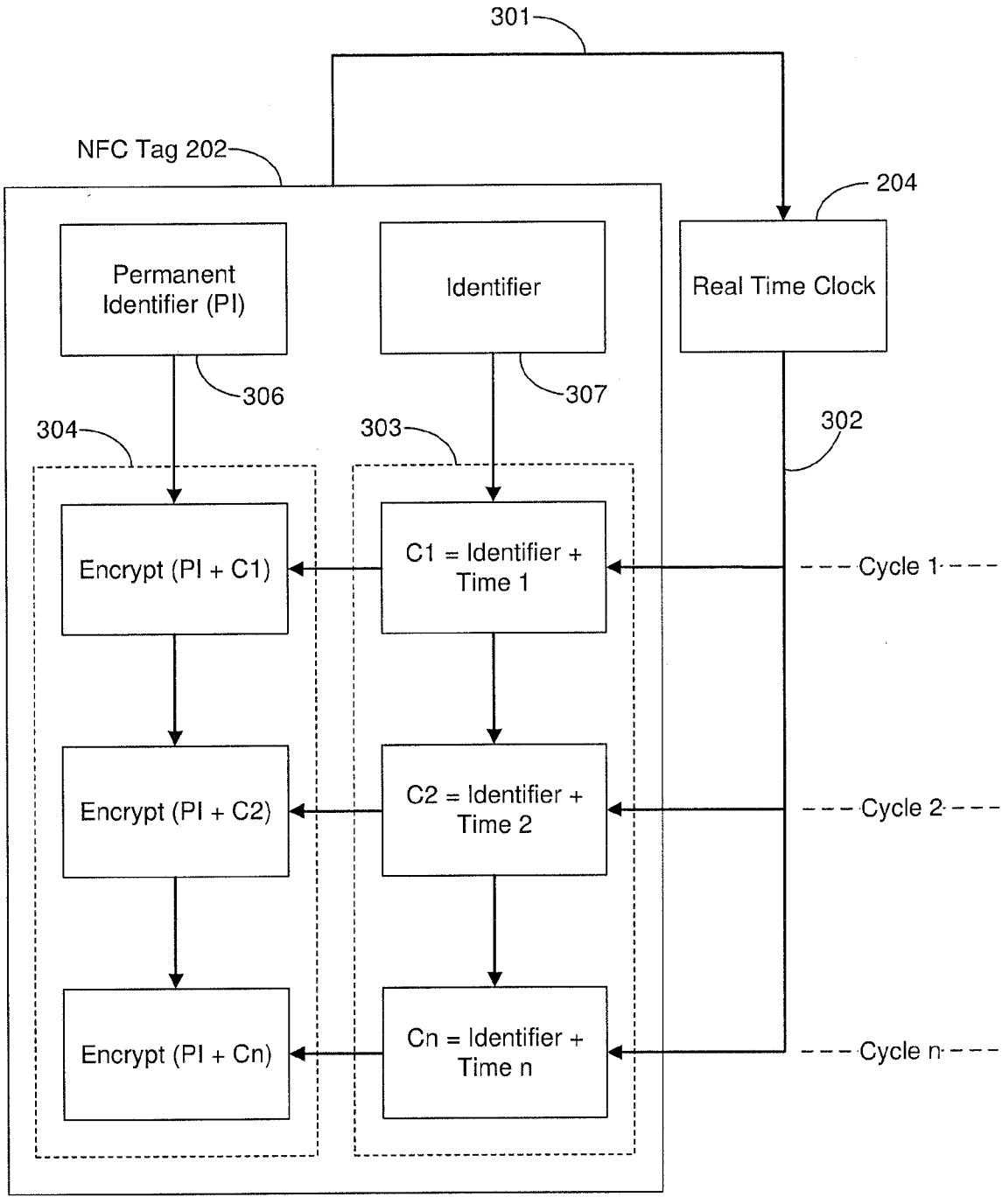
301
NFC Tag 202
204
Permanent Identifier (PI)
Identifier
Real Time Clock
306
307
304
303
302
Encrypt (PI + C1)
C1 = Identifier + Time 1
Cycle 1
Encrypt (PI + C2)
C2 = Identifier + Time 2
Cycle 2
Encrypt (PI + Cn)
Cn = Identifier + Time n
Cycle n

FIGURE 3B

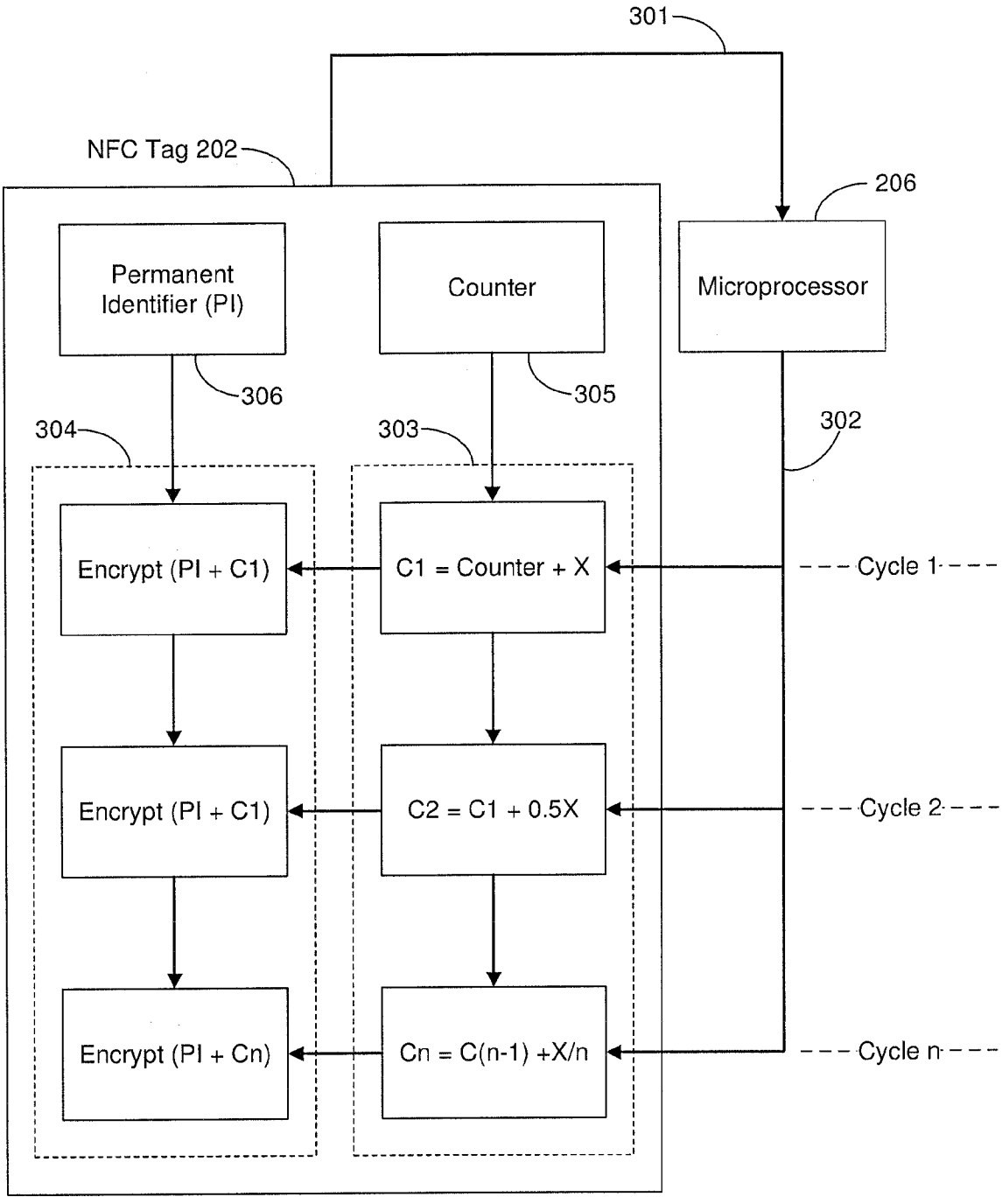
301
NFC Tag 202
206
Permanent Identifier (PI)
Counter
Microprocessor
306
305
304
303
302
Encrypt (PI + C1)
C1 = Counter + X
Cycle 1
Encrypt (PI + C1)
C2 = C1 + 0.5X
Cycle 2
Encrypt (PI + Cn)
Cn = C(n-1) +X/n
Cycle n

FIGURE 3C

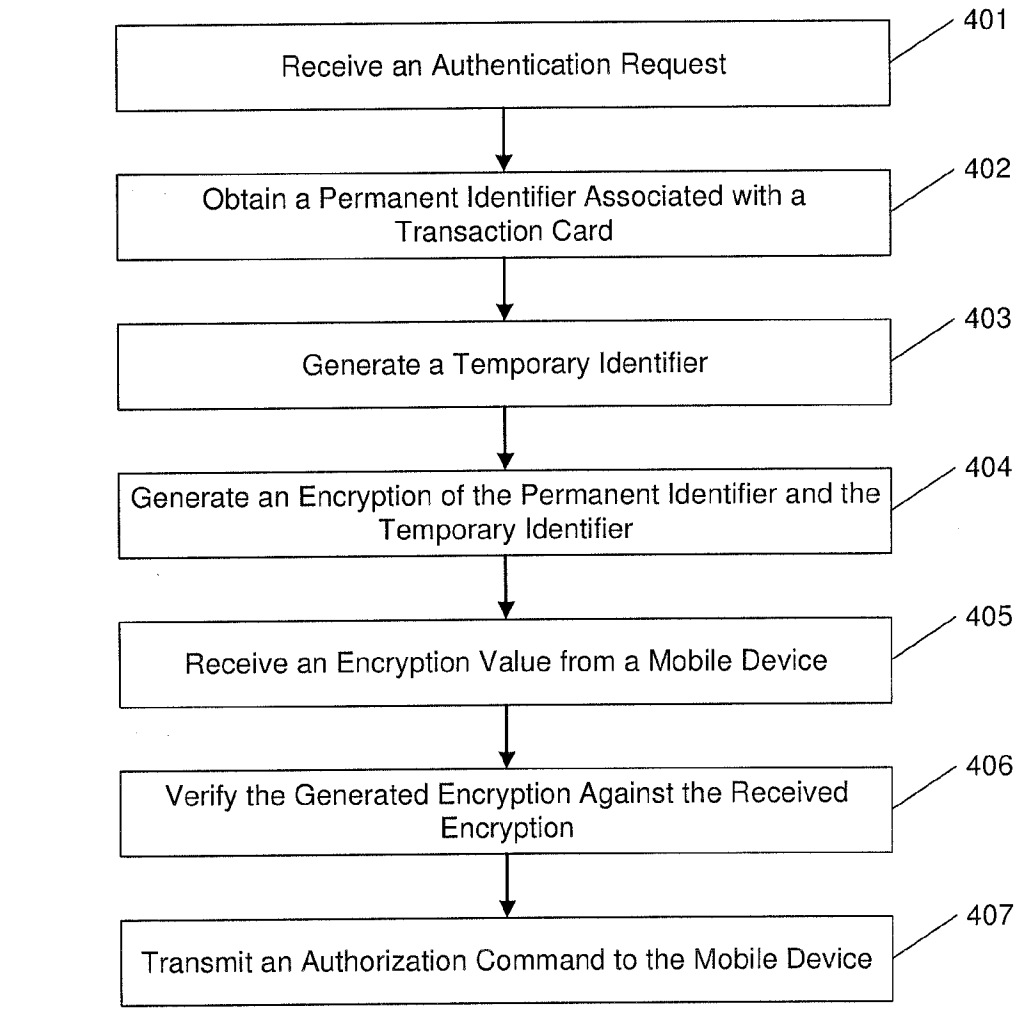
400
Receive an Authentication Request
401
Obtain a Permanent Identifier Associated with a Transaction Card
402
Generate a Temporary Identifier
403
Generate an Encryption of the Permanent Identifier and the Temporary Identifier
404
Receive an Encryption Value from a Mobile Device
405
Verify the Generated Encryption Against the Received Encryption
406
Transmit an Authorization Command to the Mobile Device
407

FIGURE 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/038487

A. CLASSIFICATION OF SUBJECT MATTER

IPC: G07F 7/10, 7/08; G06Q 20/34, 20/40, 20/04
CPC: G07F 7/1008, 7/08; G06Q 20/341, 20/40, 20/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

CPC: CPC: G07F 7/1008, 7/08; G06Q 20/341, 20/40, 20/04/ IPC: G07F 7/10, 7/08; G06Q 20/34, 20/40, 20/04

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

US-PGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB: temporary, identifier, near, clock, generator, card, rfid, and, dynamic, frequency, private, tag, polymorphic, counter, NFC, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/0302409 A1 (MALEK ET AL.) 22 October 2015 (22.10.2015), See entire documents.	1-20
A	US 2013/0200999 A1 (SPODAK ET AL.) 08 August 2013 (08.08.2013), See entire documents.	1-20
A	US 2013/0099587 A1 (LOU ET AL.) 25 April 2013 (25.04.2013), See entire documents.	1-20
A	US 2011/0211219 A1 (BRADLEY ET AL.) 02 September 2011 (02.09.2011), See entire documents.	1-20
A	US 2011/0208658 A1 (MAKHOTIN) 25 August 2011 (25.08.2011), See entire documents.	1-20
A	US 20120150737 A1 (ROTTINK ET AL.) 14 June 2012 (14.06.2012), See entire documents.	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 July 2019 (26.07.2019)	30 JUL 2019
Name and mailing address of the ISA/US **COMMISSIONER FOR PATENTS MAIL STOP PCT, ATTN: ISA/US P.O. BOX 1450 ALEXANDRIA, VA 22313-1450, UNITED STATES OF AMERICA** Facsimile No. **(571)273-8300**	Authorized officer **HARRY C. KIM** Telephone No. **571-272-4300**